Department of Homeland Security Daily Open Source Infrastructure Report for 07 July 2006

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

Daily Highlights

- The Washington Post reports that under a rule proposed by the Federal Aviation Administration, many private pilots would have to complete an Internet−based training course before being allowed to fly near restricted airspace in the Washington, DC region. (See item 13)

- The U.S. Department of Homeland Security has announced that nearly $400 million in Fiscal Year 2006 grants will be made available to strengthen the nation's ability to prevent, protect against, respond to and recover from terrorist attacks, major disasters, and other emergencies that could impact this country's critical infrastructure. (See item 21)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *July 03, Utility Automation & Engineering* — **Nashville Electric Service Website provides outage map.** When the power goes out, Nashville Electric Service (NES) customers turn to one of the most popular features on the NES Website: an online outage map with live, continuously updated outage information. Teresa Corlew, NES spokesperson says, "It's been a hit with our customers and the media who depend on the information to be accurate and timely." The map provides information during a power failure. Users can view all outages across the NES service

area or narrow their search to a specific neighborhood. They can see the number of customers who are experiencing outages, the streets that are affected, and if crews have been assigned to the problem. Information is updated every 10 minutes. NES tracks the number of visitors to the Website. NES had over 2,700 unique visits to the outage map on August 30 when Hurricane Katrina hit the Gulf Coast. The number of visits normally averaged less than 500. NES experienced a similar spike in April 2006 when tornados ripped through Middle Tennessee and left 17,000 customers without power.
Source: http://uaelp.pennnet.com/Articles/Article_Display.cfm?ARTICL E_ID=259168&p=22

[Return to top]

Chemical Industry and Hazardous Materials Sector

2. *July 06, Memphis Democrat (MO)* — **Propane leak prompts closure of city square in Missouri.** The northwest corner of the Memphis square was temporarily shut down on Monday afternoon, July 3, when a neighbor reported a gas leak at the Jackson Auction Service building in Memphis, MO. Occupants in the adjoining buildings were notified of the situation with the recommendation to temporarily evacuate the immediate area. Fire trucks were used to blockade traffic away from the area.
   Source: http://memphisdemocrat.com/2006/news/060706_gas.shtml

3. *July 06, Associated Press* — **Train with chlorine gas derails in Pennsylvania.** Nearly a dozen homes in Hershey, PA, were evacuated after a Norfolk Southern freight train carrying chlorine gas derailed near a golf course. Officials reported no injuries and no hazardous leaks but said Thursday, July 6, that the homes would remain evacuated while the 13 derailed cars were being removed. The Hershey American Legion post and part of the Hershey Country Club golf course were also evacuated.
   Source: http://hosted.ap.org/dynamic/stories/F/FREIGHT_TRAIN_DERAILS ?SITE=AP&SECTION=HOME&TEMPLATE=DEFAULT

4. *July 05, NBC 25 (MD)* — **Propane leak shuts down parts of western Maryland county.** A portion of Garrett County, MD, was shut down for more than nine hours after a gas leak was reported Wednesday morning, July 5. The leak developed when the 1,000 gallon propane tank was damaged by a piece of construction. Maryland State Police evacuated a 300−foot perimeter, including eleven businesses near McHenry Plaza. Surrounding streets were also blocked off.
   Source: http://www.nbc25.com/main/modules/news/article.php?storyid=2 856

[Return to top]

Defense Industrial Base Sector

5. *July 06, Aviation Week* — **Space radar program is focus of effort to smooth flow of classified data.** The space radar program is the first new effort in which Air Force Space Command is formulating ways to get highly classified information to front−line warfighters on a regular and timely basis, according to Maj. Gen. Mark Shackelford, the command's director of

requirements. Thousands of tactical users in Iraq and Afghanistan are often left without such information, according to Peter B. Teets, a former director of the National Reconnaissance Office (NRO). Teets, speaking at the Air Force Association's Space Warfare Symposium last week, said imagery from classified satellites can be better than commercial satellite imagery and help keep warfighters safer. He said the fact that it is often unavailable to warfighters is a "huge problem." Shackelford said the NRO is "looking at ways to streamline the delivery of information, be it imagery or whatever. The further challenge there is who you are delivering it to, and how are you delivering it."
Source: http://www.aviationnow.com/avnow/news/channel_netdefense_story.jsp?id=news/NDSP07066.xml

6. *July 06, Government Accountability Office* — **GAO−06−789R: Propulsion Systems for Navy Ships and Submarines (Correspondence).** The House Subcommittee on Projection Forces requested the Government Accountability Office (GAO) to review the Navy's assessment of alternative propulsion methods for submarines and surface combatants. GAO's objectives were to determine (1) the status and scope of key Navy studies on alternative propulsion methods, (2) the major improvements to existing propulsion systems, (3) near−term and future ships' propulsion systems, and (4) the various ship propulsion related technologies the Navy is pursuing. In March 2006, GAO provided the subcommittee with a briefing of findings regarding propulsion systems for Navy ships and submarines. This report summarizes the results of that briefing as well as additional work GAO performed since that time, and transmits the briefing slides with the updated information. Because of command changes at both the Naval Sea Systems Command and the Office of the Chief of Naval Operations and other factors, the Navy has not completed two ongoing studies. As a result, GAO was not able to assess the results of these studies.
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−789R

7. *July 05, Congress Daily* — **Defense contractors gear up to fight foreign metals ban.** A high−stakes battle affecting the fortunes of the defense and electronics industries will intensify later this month when the House and Senate Armed Services committee negotiators begin conference talks on the fiscal 2007 defense authorization bill. At issue is whether defense manufacturers can buy certain metals, such as titanium and zirconium, from foreign contractors, or if they must rely solely on domestic suppliers for the in−demand products. Worried industry trade groups, whose member companies have long been able to circumvent a law requiring the content of specialty metals be 100 percent domestically produced, have been gearing up lobbying campaigns aimed at ensuring any conference agreement will not change the status quo. Their activism has been prompted partly by the Department of Defense, which began stepping up enforcement of the law, known as the Berry Amendment, in the last year despite past indifference toward industry infractions involving minor equipment parts.
Source: http://www.govexec.com/story_page.cfm?articleid=34472&dcn=to daysnews

[Return to top]

Banking and Finance Sector

8. *July 07, Websense Security Labs* — **Multiple phishing alert: Commercial Bank of Dubai, UBS, Oxford Federal Credit Union.** Websense Security Labs has received reports of a new

phishing attack that targets customers of the Commercial Bank of Dubai. Users receive a spoofed e−mail message, which claims that a banking security alert update is available to view online. The e−mail contains a link to the phishing site that requests the user's logon ID and password. A new phishing attack that targets customers of UBS sends users a spoofed e−mail message, which claims that their account has been locked, and that they must logon to restore access to their online banking service. The message provides a link to a phishing Website that requests logon and account details. Another new phishing attack targets customers of Oxford Federal Credit Union. Users receive a spoofed e−mail message, which claims that the users' online banking services need to be renewed or their online services will be deactivated. The message provides a link to a phishing Website that requests users to log on and provide account details.
Phishing e−mail screenshots: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =540
http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =541
http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =542
Source: http://www.websensesecuritylabs.com

9. *July 06, Associated Press* — **Western Union blocks Arab cash transfers.** Money transfer agencies have delayed or blocked thousands of cash deliveries on suspicion of terrorist connections simply because senders or recipients have names like Mohammed or Ahmed, company officials said. Western Union Financial Services and MoneyGram International said their clerks are simply following U.S. Treasury Department guidelines that scrutinize cash flows for terrorist links. Most of the flagged transactions are delayed for a few hours. Some are blocked entirely. U.S. Treasury spokesperson Molly Millerwise said foreign banks have used the department's list of terrorist names to freeze $150 million in assets since September 11. The list of names, available on the Treasury's Office of Foreign Assets Control Website, contains hundreds of Mohammeds.
Source: http://biz.yahoo.com/ap/060706/emirates_muslim_money_lh1.htm l?.v=1

10. *July 05, TechWeb* — **New Trojan can change IP addresses.** A new Trojan is on the loose that enables attackers to reroute users to phony Websites −− even when the user types the URL out manually. The Trojan, dubbed DNSChanger.eg, corrupts the process of translating a domain name into an IP address, according to security researchers at security software vendor MicroWorld Technologies, which discovered the vulnerability. The exploit has "high risk potential," the researchers say. When a user types in a URL, the smart Trojan changes the "NameServer" registry key value to a fraudulent IP address. Phishers can design the fraudulent page to look very much like the pages of the site they are defrauding −− such as a bank or retailer −− and fool the user into typing in their account information. "Phishing usually requires you to be lured through emails that lead you to impostor Websites, but this requires nothing of that sort," says Govind Rammurthy of MicroWorld Technologies.
Source: http://www.darkreading.com/document.asp?doc_id=98493

[Return to top]

Transportation and Border Security Sector

11.

July 06, Department of Transportation — **Department of Transportation Secretary Norman Mineta resigning July 7.** On Thursday, July 6, Department of Transportation Secretary Norman Mineta gave the final speech of his tenure to the U.S. Chamber of Commerce in Washington, DC. He discussed the future of transportation in the 21st century. With all the changes that will come, he stressed that, "security is, and must always remain, a foremost concern." Mineta is stepping down from his job as Secretary of the Department of Transportation, effective Friday, July 7. Mineta served ten terms in Congress from California and is the only Democrat in President Bush's Cabinet,
Mineta's letter of resignation: http://www.dot.gov/aaffairs/MinetaLetter.pdf
Source: http://www.dot.gov/affairs/mineteasp070606pm.htm

12. *July 06, Associated Press* — **Empty commuter train derails in Manhattan causing delays.** An empty commuter train car derailed early Thursday, July 6, outside a tunnel leading to Pennsylvania Station in New York, causing delays and service cancellations at the height of morning rush hour. The Long Island Rail Road (LIRR) car came off the tracks around 4:30 a.m. EDT at one end of a rail yard on Manhattan's West Side. The car had not tipped over, but was positioned at an angle across several tracks, blocking trains parked inside the yard, LIRR spokesperson Sam Zambuto said. The derailment delayed trains up to 30 minutes on parts of the LIRR system, which carries an average of 274,000 people each weekday.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/07/06/AR2006070600295.html?sub=AR

13. *July 06, Washington Post* — **FAA plans training for restricted airspace.** Many private pilots would have to complete an Internet−based training course before being allowed to fly near restricted airspace in the Washington, DC region, under a rule proposed on Wednesday, July 5, by the Federal Aviation Administration (FAA). There are two restricted flight areas in the Washington region: an inner ring, which is close to downtown, and a large outer ring. Together, the zones cover about 4,200 square miles and stretch from rural Virginia to Baltimore. FAA officials said there have been more than 1,000 violations since the outer ring was established as a temporary measure in early 2003. The incursions drain resources from air−traffic controllers and from military and law enforcement authorities, officials said. In several instances, Air Force jets or law enforcement helicopters were scrambled to intercept violators. The rule would require pilots to take a course on the FAA Safety Program Website before they intend to fly under visual flight rules within about 115 miles of the District. The proposal would mostly affect the pilots of small planes or business jets.
Website: http://www.faasafety.gov/
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/07/05/AR2006070501730.html

[Return to top]

Postal and Shipping Sector

Nothing to report.

[Return to top]

Agriculture Sector

14. *July 06, Indiana Ag Connection* — **Indiana reaches milestone in premise identification.** With just under 60 days still ahead before a statewide livestock premise registration deadline, Indiana has reached a milestone: 10,000 premises have been registered with the State Board of Animal Health (BOAH). Those 10,000 premises represent nearly half of the estimated number of sites that must be part of the system by September 1, according to Jen Greiner, director for identification programs for BOAH. Indiana has approximately 23,000 premises that must meet the registration requirement. That includes all premises associated with the sale, purchase and/or exhibition of sheep, goats, cattle, swine and captive cervids.
Source: http://www.indianaagconnection.com/story−state.cfm?Id=452&yr =2006

15. *July 04, Herald−Mail (Pennsylvania)* — **Plum pox virus found in quarantined area in Pennsylvania.** A peach tree in a commercial grove in Adams, PA, has been found to have the plum pox virus, the first such finding of the year, the state Department of Agriculture said. "Our surveyors have found the first positive commercial orchard tree this year. It's located in the quarantined area of Menallen Township, Adams County," Agriculture Secretary Dennis Wolff said. "A single tree in an eight−acre block of peach trees has tested positive for the virus, and only one grower is affected. In total, 15 acres of stone fruit trees will have to be removed as a result of the detection." Plum pox virus severely decreases fruit production.
Plum Pox Virus information: http://sharka.cas.psu.edu/
Source: http://www.herald−mail.com/?module=displaystory&story_id=141 754&format=html

[Return to top]

Food Sector

16. *July 04, Food and Agriculture Organization* — **Developing nations expanding their food production.** Production and consumption of farm products are expanding faster in developing countries than in developed economies. However, a new joint report from the United Nations' Food and Agriculture Organization and Organization for Economic Cooperation and Development reports productivity growth in the world's poorest nations is not keeping pace with the food needs of their rising populations. Because of this, the poorest developing countries will be increasingly dependent on world markets for their food security and also more vulnerable to price fluctuations in world markets, the report relays.
Source: http://www.fao.org/newsroom/en/news/2006/1000349/index.html

[Return to top]

Water Sector

17. *July 05, U.S. Environmental Protection Agency* — **Drinking water programs funded.** States, territories and tribes will share more than $940 million from three U.S. Environmental Protection Agency (EPA) grant programs to support the quality and security of the nation's drinking water. The water supplies for more than 270 million people will benefit from the funding. More than $837 million will support Drinking Water State Revolving Funds programs,

which help states, territories and tribes finance infrastructure improvements to public water systems. Federal capitalization grants fund low−interest loans to public water systems. Eligible projects include upgrades to treatment facilities, certain storage facilities and distribution systems. Another $98 million in grants will fund the Public Water Supervision System. This system operates under the Safe Drinking Water Act and provides resources to implement and enforce drinking water regulations and programs. Finally, EPA will provide five million dollars in FY 2006 counter−terrorism grants to states and territories. The grants will help provide drinking water utilities with technical assistance and training to improve the readiness of first responders at drinking water systems, including practicing emergency response and recovery plans. States are also encouraged to develop strategies to help utilities implement security enhancements.
Source: http://yosemite.epa.gov/opa/admpress.nsf/27166bca9a9490ee852570180055e350/926a24fac132b7d8852571a2004eca0e!OpenDocument

[Return to top]

Public Health Sector

18. *July 06, Agence France−Presse* — **Thailand hopes to be bird−flu free in three years.** Thailand hopes to be completely free of the H5N1 bird flu virus in three years, after eight months so far without an outbreak, the agriculture minister has said. "Thailand can effectively control the bird flu virus. We have been free of the virus for 239 days, while neighboring countries are still reporting outbreaks," Agriculture Minister Sudarat Keyuraphan said. "If we are able to control the virus for the rest of this year, we will have fewer worries next year, and I am confident that Thailand will be free from the bird flu virus within three years," she said. Thailand has suffered 22 cases of bird flu in humans, including 14 fatalities, most recently in December. Thailand has recruited 900,000 volunteers around the country to help control the virus. Every three months, they fan out across the country to spray disinfectant around poultry farms and to check for any signs of illness among residents.
Source: http://news.yahoo.com/s/afp/20060706/hl_afp/healthfluthailand_060706135910;_ylt=AlV6a_g_iatI1cu5yfh.bi.JOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

19. *July 06, Reuters* — **Flu often unrecognized in children.** Doctors often fail to diagnose the flu in young children, according to a new study that supports vaccinating youngsters. Researchers found that 5.6 percent of children under age five living around Nashville, TN, Cincinnati, OH, and Rochester, NY, had the flu during the 2002−2003 winter season. The following year, the number more than doubled to 12.2 percent, according to the study. But doctors made the correct flu diagnosis less than 28 percent of the time.
Abstract: http://content.nejm.org/cgi/content/short/355/1/31
Source: http://news.yahoo.com/s/nm/20060705/hl_nm/flu_dc;_ylt=AhCacjEK0Pj7aYKinDKwVJEQ.3QA;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

20. *July 04, Chennai Online News* — **Over one thousand affected by chikungunya.** As many as 1,049 persons have been affected by chikungunya disease in Dharmapuri district of Tamil Nadu, India, collector M. Chandrashekharan said Tuesday, July 4. Talking to reporters, he said 698 persons had been affected in rural areas and 351 in urban limits. Blood samples have been

sent to the Central Virological Laboratory for further tests. No casualty has been reported so far, the collector said. As many as 1,685 committees have been formed to create awareness among the people of the district by conducting door−to−door verification.
Chikungunya information: http://www.phac−aspc.gc.ca/msds−ftss/msds172e.html
Source: http://www.chennaionline.com/colnews/newsitem.asp?NEWSID=%7B 17CBAF09−33CA−4DBD−BF48−6155A196D13E%7D&CATEGORYNAME=Tamil+N adu

[Return to top]

Government Sector

21. *July 06, Department of Homeland Security* — **DHS announces grants to secure the nation's critical infrastructure.** The U.S. Department of Homeland Security (DHS) announced on Thursday, July 6, that nearly $400 million in Fiscal Year 2006 grants will be made available to strengthen the nation's ability to prevent, protect against, respond to and recover from terrorist attacks, major disasters and other emergencies that could impact this country's critical infrastructure. The funding will be dispersed through the DHS Office of Grants and Training's Infrastructure Protection Program. "The Infrastructure Protection Program provides the means to move forward in developing sustainable, risk−based critical infrastructure security initiatives for man−made and natural threats that could potentially have devastating impacts on the economy and communities throughout the nation," said DHS Under Secretary for Preparedness George Foresman. The infrastructure grants will be divided among seven programs that constitute major critical infrastructure sectors ranging from transportation modes to the nation's ports. Allocation totals have been determined for five of the programs: Transit Security Grant Program (intracity rail, bus, and ferry systems), Buffer Zone Protection Program, Chemical Sector Buffer Zone Protection Grant Program, Intercity Passenger Rail Security Grant Program, and the Trucking Security Program.
For information on allocations and eligible applicants visit the Office of Grants and Training: http://www.ojp.usdoj.gov/odp/grants_programs.htm
Source: http://www.dhs.gov/dhspublic/interapp/press_release/press_re lease_0942.xml

[Return to top]

Emergency Services Sector

22. *July 06, Federal Emergency Management Agency* — **Movies of California earthquakes help preparedness.** Scientists at the California Institute of Technology can now create a movie just 45 minutes after a temblor, showing how seismic waves spread from the epicenter. During a recent demonstration, the staff at the Caltech's Seismological Laboratory played a movie of the 2003 magnitude−5.1 Big Bear earthquake. The information could help Southern California residents better understand how temblors behave and whether they will be affected by the ground shaking.
The public can access movies for Southern California temblors of magnitude 3.5 and higher at: http://shakemovie.caltech.edu/
Source: http://www.fema.gov/emergency/reports/2006/nat070606.shtm

23. *July 05, Federal Emergency Management Agency* — **President declares major disaster for Delaware.** The head of the Department of Homeland Security's Federal Emergency Management Agency (FEMA) announced that federal disaster aid has been made available for the State of Delaware to supplement state and local recovery efforts in the area struck by severe storms and flooding that began on June 23, and continuing.
For more information: http://www.fema.gov/news/event.fema?id=6525
Source: http://www.fema.gov/news/newsrelease.fema?id=27443

24. *July 05, Courier−Post (NJ)* — **New Jersey county fixing communication glitches.** Burlington County, NJ, officials have taken quick action to correct communications shortcomings with local agencies in a recent emergency response exercise intended to combat a health epidemic. During the exercise, the township had to rely on faxes to communicate with the county, said William Lowe, emergency management coordinator for Tabernacle. To remedy those deficiencies, the county board of freeholders has given the five participating Pinelands municipalities $25,000 worth of electronic equipment. Freeholder−Director James Wujcik presented the emergency management coordinators from Bass River, Shamong, Tabernacle, Washington Township and Woodland with laptop computers, computer printers, fax machines, projectors and BlackBerry communication devices. County health coordinator Robert Gogats said the equipment will better link the towns and the county.
Source: http://www.courierpostonline.com/apps/pbcs.dll/article?AID=/20060705/NEWS01/607050344/1006

25. *July 05, Times−Picayune (LA)* — **Nation's 911 systems: Due for an overhaul.** While Louisiana's Statewide Interoperable Communication System Executive Committee is making progress setting up new radio communications for state and local rescue teams, it has not discussed how the public could send text or e−mail messages for emergencies. Michael Abiatti, chairman of the committee, said he is trying to figure out how it could be done. A new system to receive the messages would need the components, capacity and know−how among operators to make it work. The National Emergency Number Association has launched an effort called Next Generation E911 to examine the shortcomings of response mechanisms to emergency messages from cell phones by text message, automobile satellite−link radio systems, the Internet and voice phone systems over the Internet. "While the existing 911 system has been a success story for more than 30 years, it has been stretched to its limit as technology advances," according to an association report. "Unfortunately, the current 911 system was never intended to receive calls and data from these new and emerging technologies. As a result, it is being asked to perform functions it was not designed to handle. In short, the nation's 911 systems are in need of a significant overhaul."
Source: http://www.nola.com/news/t−p/frontpage/index.ssf?/base/news−6/1152079275187350.xml&coll=1

26. *July 05, New Mexican* — **New Mexico emergency officials fear they can't overcome call system's hang−ups.** Unprecedented use of the region's reverse−911 system by the Santa Fe, NM, Regional Emergency Communications Center last month highlighted local officials' concerns about how they can get the word out to area residents during an emergency. Calls to 2,826 Eldorado residences June 7 far exceeded the number of people officials had previously tried to reach with the system. Fewer than 600 answered the call. Some identified issues with this incident: 1,845 answering machines, caller−identification systems that block automated

calls, and residents that just hung up. Emergency operators now know to listen to their recorded messages before they put them on the automated−dialing system. Other problems resulted from operators' uncertainty over how the system operated. It called names starting with letters A, B, and C, and then an operator restarted it, not sure it had activated. It called those numbers again but then stopped as a result of an automated time−out process. Now operators know to override the 30−minute cutoff when calling thousands of numbers. The incident also confirmed what emergency officials already knew: the system might not be sufficient to reach all area residents in the event of a major disaster.
Source: http://www.freenewmexican.com/news/45953.html

[Return to top]

Information Technology and Telecommunications Sector

27. *July 06, IDG News Service* — **Hacker promises month of browser holes.** The creator of a widely used hacking tool has promised to publish details of one browser security hole per day during July. HD Moore, the hacker behind the Metasploit toolkit, started his Month of Browser Bugs on July 1 by publishing software that demonstrates bugs in a variety of Web browsers. Moore said he decided to do the month of bugs in order to show the kinds of results he's generated using a variety of automated security testing tools known as "fuzzers."
Source: http://www.techworld.com/news/index.cfm?newsID=6383&printerf riendly=1

28. *July 06, Washington Post* — **Consultant breached FBI's computers.** A government consultant, using computer programs easily found on the Internet, managed to crack the FBI's classified computer system and gain the passwords of 38,000 employees, including that of FBI Director Robert S. Mueller III. The break−ins, which occurred four times in 2004, gave the consultant access to records in the Witness Protection Program and details on counterespionage activity, according to documents filed in U.S. District Court in Washington. As a direct result, the bureau said it was forced to temporarily shut down its network and commit thousands of man−hours and millions of dollars to ensure no sensitive information was lost or misused. The government does not allege that the consultant, Joseph Thomas Colon, intended to harm national security. But prosecutors said Colon's "curiosity hacks" nonetheless exposed sensitive information. Colon, an employee of BAE Systems who was assigned to the FBI field office in Springfield, IL, said in court filings that he used the passwords and other information to bypass bureaucratic obstacles and better help the FBI install its new computer system. And he said agents in the Springfield office approved his actions.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/07/05/AR2006070501489_pf.html

29. *July 06, VNUNet* — **Symantec mistakes open source tool for Trojan.** A faulty update has caused Symantec to incorrectly detect the Zlob Trojan in the legitimate open source Nullsoft Scriptable Install System (NSIS) tool. The false positives appear to be caused by a faulty update of Symantec's antivirus signatures distributed on July 1. According to user comments, the problem was repaired on Monday, July 3. The faulty detection caused the antivirus software to remove or quarantine the allegedly infected files. The problems only occurred with version 2.17 of NSIS.
Source: http://www.vnunet.com/vnunet/news/2159763/symantec−mistakes− open−source

30. *July 05, Security Focus* — **Apple Safari Web Browser DHTML SetAttributeNode() null dereference denial−of−service vulnerability.** Apple Safari Web browser is prone to a denial−of−service vulnerability. Analysis: An attacker can exploit this issue to crash an affected browser.
Vulnerable: Apple Safari 2.0.4.
Solution: Currently, Security Focus is unaware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/18822/references

31. *July 05, Security Focus* — **Microsoft Internet Explorer Href Title denial−of−service vulnerability.** Microsoft Internet Explorer is prone to a denial−of−service vulnerability. Analysis: An attacker can exploit this vulnerability to cause the application to stop responding, denying service to legitimate users.
For a complete list of vulnerable products: http://www.securityfocus.com/bid/18820/info
Solution: Currently, Security Focus is not aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/18820/references

32. *July 05, Security Focus* — **Microsoft Excel unspecified remote code execution vulnerability.** Microsoft Excel is prone to an unspecified remote code−execution vulnerability. Analysis: Successfully exploiting this issue allows attackers to execute arbitrary code in the context of targeted users. Attackers are actively exploiting this vulnerability in targeted attacks and to install malicious software.
For a complete list of vulnerable products: http://www.securityfocus.com/bid/18422/info
Solution: Microsoft has released a security advisory addressing this issue. Official fixes are not currently available.
Microsoft Security Advisory: http://www.microsoft.com/technet/security/advisory/921365.mspx
Source: http://www.securityfocus.com/bid/18422/references

33. *July 05, Security Focus* — **Adobe Reader multiple unspecified security vulnerabilities.** Adobe Reader is susceptible to multiple unspecified security vulnerabilities. Analysis: Due to the "critical" rating given by the vendor, combined with their "Severity rating system," at least one of these vulnerabilities may be exploited to execute arbitrary machine code in the context of the affected application.
For a complete list of vulnerable products: http://www.securityfocus.com/bid/18445/info
Solution: Adobe has released updated software to address these issues. For information on obtaining and applying fixes: http://www.securityfocus.com/bid/18445/references
Source: http://www.securityfocus.com/bid/18445/discuss

34. *July 05, ZDNET News* — **HP to hack customers' networks.** Hewlett−Packard (HP) is taking a cue from hackers to help protect corporate systems. The company plans to launch a penetration−testing service for businesses in October that will use the same techniques as hackers to gain access to its customers' machines. However, the exploit code it will use will be controlled and will not propagate itself as a worm would, HP said on Tuesday, July 4. The HP Active Countermeasures (HPAC) service will use a single server and between eight and 10 scanning clients per 250,000 connected devices. Each of the clients will be given a range of Internet Protocol addresses to scan, and will move through the range scanning for particular

flaws.
Source: http://news.zdnet.com/2100−1009_22−6090825.html

35. *July 05, Palladium−Item (IN)* — **Verizon outage impacts thousands.** About 22,000 Verizon customers in the Richmond, IN, area were without service Wednesday afternoon, July 5, when excavating crews working near the Interstate 70 and U.S. 27 interchange damaged one of Verizon’s major fiber optic lines. The outage also knocked out Randolph County’s 911 system.
Source: http://www.pal−item.com/apps/pbcs.dll/article?AID=/20060705/ NEWS01/60705004

36. *June 06, Government Accountability Office* — **GAO−06−476: Telecommunications: Full Adoption of Sound Transition Planning Practices by GSA and Selected Agencies Could Improve Planning Efforts (Report).** With the current governmentwide telecommunications contracts set to expire, the General Services Administration’s (GSA) Federal Technology Service (FTS) and its customer agencies must prepare to transition their services to a new contract vehicle. The previous federal effort to transition telecommunications services proved to be a large, complex task. The Government Accountability Office (GAO) was asked to determine to what extent (1) selected agencies used sound practices in preparing for the transition and (2) GSA’s FTS has prepared for the transition by addressing previous lessons learned and providing agencies with guidance on sound transition planning. GAO recommends that the Attorney General and the Secretary of Energy perform the analyses necessary to identify required transition resources for their agencies. In addition, GAO recommends that the Administrator of General Services provide guidance to GSA’s customer agencies that reflects all of the sound transition planning practices. In commenting on a draft of this report, GSA, the Department of Justice, the Department of Energy, and the Department of the Interior generally agreed with GAO's recommendations.
Highlights: http://www.gao.gov/highlights/d06476high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−476

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of publicly available exploit code for two unpatched vulnerabilities in Microsoft Internet Explorer. By persuading a user to double click a file accessible through WebDAV or SMB, a remote attacker may be able to execute arbitrary code with the privileges of the user. US−CERT is tracking the first vulnerability as VU#655100:
http://www.kb.cert.org/vuls/id/655100

The second issue is a cross domain violation vulnerability that is being tracked as VU#883108: http://www.kb.cert.org/vuls/id/883108

Successful exploitation could allow a remote attacker to access the contents of a web page in another domain. This exploitation could lead to information disclosure, which may include harvesting user credentials. Until an update, patch, or more information becomes available, US−CERT recommends the following:

Do not follow unsolicited links.

To address the cross domain violation vulnerability (VU#883108):
http://www.kb.cert.org/vuls/id/883108

Disable ActiveX as specified in the Securing Your Web Browser:
http://www.us−cert.gov/reading_room/securing_browser/#Intern et_Explorer

Review Malicious Web Scripts FAQ:
http://www.cert.org/tech_tips/malicious_code_FAQ.html#steps

US−CERT will continue to update current activity as more information becomes available

Public Exploit Code for Unpatched Vulnerability in MS Office Hyperlink Object Library

US−CERT is aware of publicly available exploit code for an unpatched buffer overflow vulnerability in Microsoft Hyperlink Object Library (HLINK.DLL). By persuading a user to access a specially crafted hyperlink in an email message or MS Office document, a remote attacker may be able to execute arbitrary code with the privileges of the user.More information about this vulnerability can be found in the following:

VU#394444 − Microsoft Hyperlink Object Library stack buffer overflow:
http://www.kb.cert.org/vuls/id/394444

Until an update, patch, or more information becomes available, US−CERT recommends the following:

Do not follow unsolicited web links received in email messages or embedded in MS Office documents.

US−CERT will continue to update current activity as more information becomes available.

PHISHING SCAMS
US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT.

http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online.
http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 37501 (−−−), 445 (microsoft−ds), 47610 (−−−), 38566 (−−−), 54856 (−−−), 26777 (−−−), 24232 (−−−), 56881 (−−−), 25 (smtp) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

37. *July 06, South Florida Sun−Sentinel* — **Florida store looted after attack with acid, fire bombs.** Robbers used acid and fire bombs to terrorize, and then loot a small Hollywood, FL, store on Pembroke Road on Thursday, July 6. Detective Carlos Negron, police spokesperson, said the owner of the A−1 Food Stop and an employee were working inside the store when they heard an explosion in front of the business. While both victims were taking cover, another bomb was thrown directly in front of the cash register, but did not detonate. A man entered the store, retrieved the device, and threatened the victims. As the man left the store with the bomb, approximate 15 to 20 men rushed into the store and looted it. When police searched the store, a Molotov cocktail was found in front of the register and the protective glass. Detectives said the fire bomb had malfunctioned and never ignited.
Source: http://www.sun−sentinel.com/news/local/broward/sfl−76hwdstor ebomb,0,7969415.story?coll=sfla−news−broward

38. *July 06, KDKA (PA)* — **All−Star Game security measures begin.** The security crackdown has begun around PNC Park and parts of downtown Pittsburgh to prepare for the All Star baseball game festivities which begin this weekend. The game itself is Tuesday evening, July 11. Twenty metal detectors are now in place at the stadium and more are on the way. Detectors are just one of the many security measures being put into place over the next few days. Concrete barriers and very tall fences are also being put into place on the North Shore to keep people safe. "Compared to when we had in 1994, it's a big difference, but it is post 9/11, so there's a lot more we have to do," said Lt. Scott Schubert of the Pittsburgh Police.
Source: http://kdka.com/topstories/local_story_186192312.html

[Return to top]

General Sector

Nothing to report.

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.